Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Managing Risk in A Program Office Environment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Bill /Shepherd	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Defense Acquisition University Alumni Association 2550 Huntington Ave, Suite 202 Alexandria, VA 22303	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**16**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

MANAGING RISK IN A PROGRAM OFFICE ENVIRONMENT

Bill Shepherd, PMP

People in program offices make decisions every day. Sometimes the alternatives are clear with unambiguous outcomes, but more often the options are less certain and have far-reaching, unintended consequences. An effective risk management program can provide program managers with the information they need to make smart decisions in the face of this uncertainty. Although the techniques for risk management are well documented and not technically difficult, a variety of factors make them hard to implement effectively. This article describes what risk management is, identifies some of the typical challenges, and provides specific examples and recommendations on how to implement an effective risk management program.

The techniques for risk management are well documented and not technically difficult. Reference material is readily available and can be found in the Defense Acquisition University (DAU) Risk Management Guide, Project Management Institute's Guide to the Project Management Body of Knowledge®, and the DAU Acquisition Reform Office Risk Management Community of Practice. The Defense Acquisition University has taught risk management and published training material on the subject for years. If it is not difficult and widely documented, then why is it so hard?

Three things make effective risk management hard.

1. It seldom seems urgent. It deals — or should deal — with events far enough in the future that there is sufficient time to influence the situation or develop alternatives. Unfortunately, less important daily pressures often get more attention.

2. It does require careful thought. People have to understand the distinction between risks, which have a degree of uncertainty associated with them, and issues, which are realities to be managed. The devil is in the details and these details must be clearly communicated to isolate the uncertainty and understand its impact. Understanding the true situation will allow teams to

focus on solving the right problem and develop far more effective mitigation plans.

3. It requires common understanding and commitment from everyone on the team. This means that risk management must be part of the organizational culture, with strong support from senior management and informed participation by the entire team. Creating that common vision and institutionalizing the processes takes training, an investment in resources, and occasional reinforcement.

Why Are Acquisition Projects "Risky"?

Acquisition programs are risky because they occur in an environment of constant change. As illustrated in Figure 1, the skills available in the workforce and those needed to support fielded technology are always moving out of alignment.

Threats, which drive requirements, are constantly changing. The end item may be obsolete by the time it is fielded unless legacy migration and technology insertion are built into the program.

Statutory and regulatory requirements and their implementing instructions are constantly changing. Industry standards and best practices are constantly evolving.

The use of new technology means historical experience is less accurate in predicting areas in which problems may occur. Training and experience may become dated as new technology becomes available.

Legacy systems often require skills that are part of the tacit knowledge gained over the years by a maturing workforce. As these workers retire or move on to second careers, this knowledge needs to be

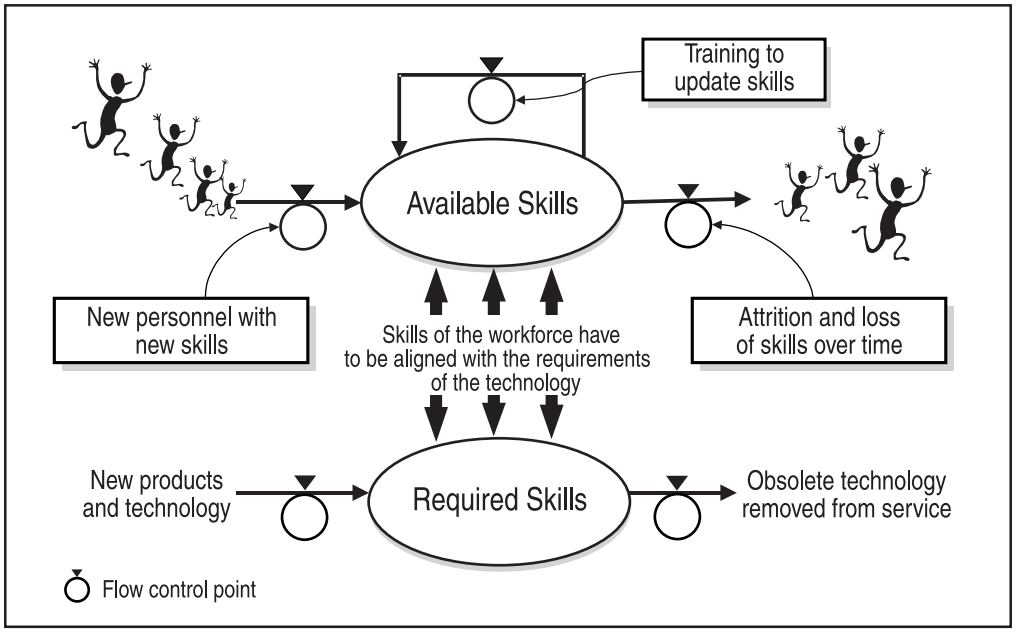


Figure 1. Aligning Personnel Skills to Technology Requirements

passed on. Workforce planning is a strategic mitigation factor for risk.

Interfaces with other efforts upon which the project depends can have a critical impact on the project's ability to deliver successfully. There is always the risk that a funding reduction in one program will have unintended consequences in another. The addition of interoperability as a Key Performance Parameter (KPP) in the Operational Requirements Document (ORD) and the requirement for a Command, Control, Communications, Computers, and Intelligence Support Plan (C4ISP) at milestone decision points are two efforts targeted at mitigating this risk.

THE RISK MANAGEMENT PROCESS

The tasks required to perform risk management can be grouped and labeled in a variety of ways. Figure 2 shows the terminology used in this article. The labels selected are not critical and even the references listed above are not consistent in their terminology. What ***is*** important is that the team understands the process so they can implement it effectively.

DEFINITIONS

Definitions make clear communication and common understanding possible. To identify the risks that require the most attention, the team needs an objective standard against which to subjectively assess both probability and impact. In the absence of an objective standard, individuals will make their own value judgments, which are tough to defend and can lead to misunderstandings.

There is no single correct set of definitions, but the ones below are targeted directly toward the problem of managing

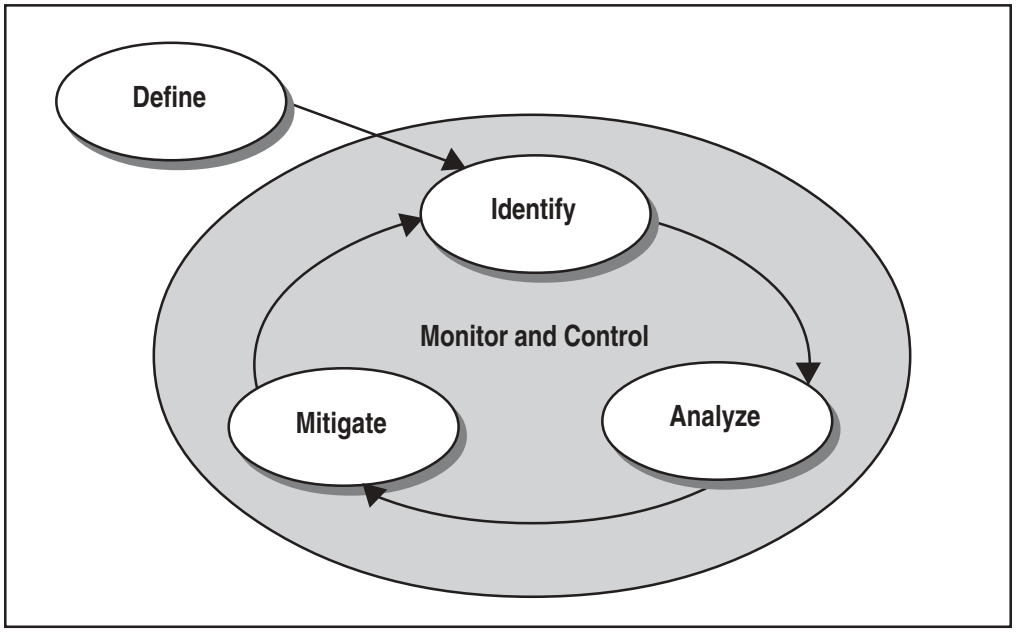


Figure 2. Risk Management Tasks

risk in a program office and therefore worth considering.

RISK

Risk exists when, in a given *situation*, there is both an *event* with a *chance* of occurring and one or more possible *outcomes* of that occurrence that will have an *impact* on the program. There are several key words in this definition that will be addressed later.

RISK MANAGEMENT

Risk management is an organized, systematic process that efficiently identifies risks, prioritizes them, develops and documents contingency plans and mitigation strategies, and provides decision-makers with the necessary information at the appropriate time to make sound decisions.

PROBABILITY

People can usually agree on a subjective probability within the bands shown in Figure 3. The break points used are one-half, one-third, and one-tenth; probabilities to which most people can relate to based on experience with coins, dice, or playing cards. A key point to note is that the assessment is made using "existing processes, infrastructure, and governance." Changes in those areas can be used to mitigate the risk.

IMPACT

Impact. If a risk event actually occurs, the result may affect cost, schedule, technical performance, or a combination of the three. These are the typical areas of risk impact but there may be others such as security or political concerns.

Probabilty			Existing Processes, Infrastructure and Governance
Near Certainty	Very High (>90%)	5	…will not avoid the risk event and there is no known alternative. (Less than 10% chance it **will not** happen.)
Highly Likely	High (67%-90%)	4	…will not avoid the risk event, but an alternative may be available. (Less than 1/3 chance it **will not** happen.)
Likely	Medium (34%-66%)	3	…may avoid this risk and an alternative may be available. (About a 50% chance it will happen.)
Unlikely	Low (11%-33%)	2	…typically avoid this type of risk with minimal oversight in similar cases. (Less than 1/3 chance it **will** happen.)
Remote	Very Low (<10%)	1	..will effectively avoid or mitigate this risk. (Less than 10% chance it **will** happen.)

Figure 3. Assessing Risk Probability

Once the areas of impact have been identified, the different levels of impact have to be quantified in each of these areas. This quantification should be linked to objective criteria whenever possible, especially if specific thresholds and objectives are provided. This can be accomplished using KPP thresholds and objectives contained in the ORD, and key milestone dates. Figure 4 shows an example of how this linkage can occur. The figure also demonstrates how program risk tolerance can be considered in setting the impact levels.

Risk tolerance is a measure of the level of risk a program is willing to accept. Figure 5 shows the result for a program with Low risk tolerance. A similar approach can be applied to cost, schedule, or any other impact area in which there is a "three-tier" relationship between the minimum acceptable, desired, and allocated or planned result.

COMMUNICATING THE PROCESS

The entire team has to understand and participate in the risk management process for it to be effective. This requires both initial training and periodic reinforcement especially when changes in personnel occur. Managing risk in different phases of the program may require different skills and focus. Depictions of the process, definitions, and standards for assessing probability and impact, should be kept simple and provided to each member of the team. Since most people usually only think about the details of risk management when they decide to nominate a risk, this guidance should be something that is easily referenced. Figure 6 shows a

	Risk Impact	
Risk Tolerance:	**Low**	**High**
Allocation		
– Meets objective with satisfactory margin, but short of allocation or design goal		1
– Meets objective with small margin, but well below allocation or design goal	1	2
Objective		
– Meets threshold with satisfactory margin, but just short of objective	2	3
– Meets threshold with small margin, but well below objective	3	4
Threshold		
– Just short of threshold	4	5
– Significantly below threshold	5	

Threshold – Minimal acceptable performance the user will accept. Will not use system if it does not meet this performance level.

Objective – Level of performance desired by the user.

Allocation – Performance assigned to a component or end item as part of the system engineering process. Usually supports achievement of objective performance criteria.

Figure 4. Linking Impact Assessments to Objective Criteria

Severity		Cost	Schedule	Functional Performance	Security/ Political/ Programmatic
Unacceptable	**5**	>20% deviation from planned budget	Cannot meet APB milestone or key program milestone	Significant shortfall to threshold requirement	
Critical	**4**	15%-20% deviation from planned budget	Major slip (over 4 months) or within 2 months of APB milestone	Nearly meets threshold requirement	
Significant	**3**	10%-15% deviation from planned budget	Slip less than 4 months in key milestones	Meets threshold with small margin, but is well short of objective	
Marginal	**2**	<10% deviation from planned budget	Slip from planned schedule of less than 1 month	Meets threshold with significant margin, but is just short of objective	
Minimal	**1**	Minimal deviation from planned budget	Minimal schedule impact	Will not cause a failure to meet objective, but short of design allocation	

Threshold – Minimal acceptable performance the user will accept. Will not use system if it does not meet this performance level.

Objective – Level of performance desired by the user.

Allocation – Performance assigned to a component or end item as part of the system engineering process. Usually supports achievement of objective performance criteria.

Figure 5. Assessing Risk Impact

simple risk management process description. This can be combined with the probability and impact descriptions in Figure 3 and Figure 5 to provide a ready reference for the team. Many programs create laminated handouts as bookmarks or that are sized for binders or wallets.

Identifying Risks — Where to Look

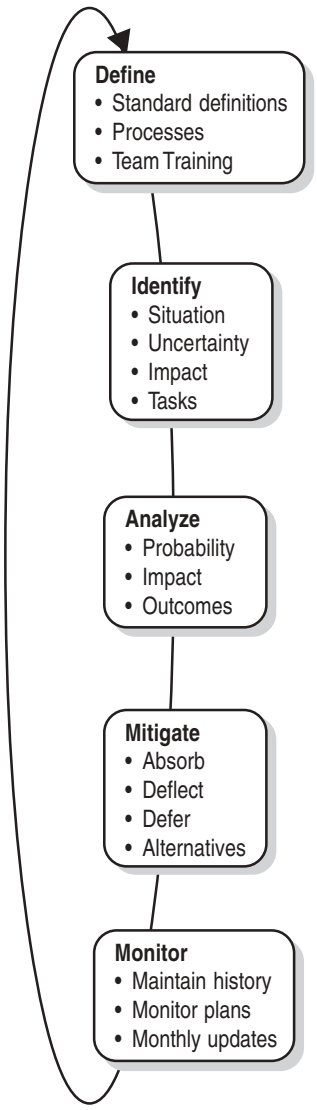
Assumptions

The first place to look for risk is in the assumptions. Any formal program brief should identify the key assumptions being made by the team, and consider the impact to the program if the assumptions prove to be false. If the combination of probability and impact exceeds the level of comfort for the leadership, then it warrants being tracked as a risk.

Work and Organizational Breakdown Structure (WBS and OBS)

The project Work Breakdown and Organizational Breakdown Structures (WBS and OBS) are useful guides for identifying risk.

The WBS should include all activities and deliverables within scope of the project,



DEFINITIONS:

- **Risk:** An uncertain (usually future) event with a definable impact on the program.
- **Risk Management:** A systematic, organized process to efficiently identify, analyze, mitigate, and track risks. It includes both minimizing the impact of unfavorable events and maximizing the benefit of favorable events.
- **Mitigation Options:** Reduce the probability that the risk event may occur, reduce the impact if it does, or increase the probability of more acceptable outcomes.
- **Contingency:** Accept that the risk event may occur and prepare to absorb the impact if it does.

RISK NOMINATION:

- **Situation** – Describe the facts that create the situation in which the risk event may occur.
- **Uncertainty** – What is the uncertain event of concern? If it is a single event, when will it occur? If it is an ongoing activity, how will we know it happened? How likely is it to occur?
- **Impact** – If the risk event occurs, how will that impact the program? If there is more than one possible outcome, assess the probability and impact for each case.
- **Tasks to Mitigate** – What actions should be taken to mitigate the risk or to develop contingency plans?

RISK MANAGEMENT BOARD DECISIONS:

- **Accept** – Formally track and assign action to develop mitigation plan.
- **Accept and Escalate** – Formally track, assign action to develop mitigation strategy, and refer to senior management due to scope of impact or potential mitigation costs.
- **Reject (Handle as Issue)** – No uncertainty exists or there is insufficient time to mitigate. Refer the issue to appropriate level of management for action.
- **Reject (Need more Information)** – Unable to determine if risk exists or requires formal monitoring. Assign action to develop more information.
- **Reject** – Does not require formal Risk Management Board attention.

Figure 6. Risk Management Process

so it is a good tool to ensure that all portions of the program are considered.

The OBS defines the functional disciplines involved. This represents a significant corporate knowledge base that can identify where the problems typically occur in a given area of expertise. Team meetings or Technical Interchange Meetings are a good time to ask "What is going to keep us from being successful on the project?"

Risk Breakdown Structure (RBS)

The concept of using a Risk Breakdown Structure (RBS) has been proposed by David Hillson (2002) to provide a

hierarchical breakdown of the sources of risk. He cites several potential uses for an RBS, including using it to provide a structure for conducting risk assessments. The top two levels of the RBS can serve as a prompt list to structure a risk brainstorming session, while lower levels can be used as a checklist to help ensure that all areas of risk are addressed. This is similar in concept to using an Ishikawa or Fishbone diagram as a brainstorming tool to classify and characterize risks. Any tool or construct that can help the team conduct a complete assessment of program risk is helpful.

Risk Analysis

Risks need to be analyzed to verify the assessment of probability and impact, and determine their relative priority. Program managers need to know where to apply limited resources to mitigate the most risk, and the cost of implementing mitigation strategies can be considerable.

Risk Classification

A nominal classification of Low, Medium, or High may be useful for a snapshot of risk status on a program, but it does not provide enough information to allocate resources. Placing risks in a risk matrix based on the assessment of probability and impact shows their relative importance (ordinal ranking), but this still does not quantify the dollarized impact to the program or justify a level of risk funding. Figure 7 shows a sample risk matrix. To fully understand the risk exposure of a program, the cost of both the impact and the mitigation options needs to be assessed. However, these assessments cost time and money and should be reserved for those risks with the greatest perceived combination of probability and impact.

What Is Expected Value and Why Should I Care?

A useful concept is the "Expected Value" of a risk, which is the product of

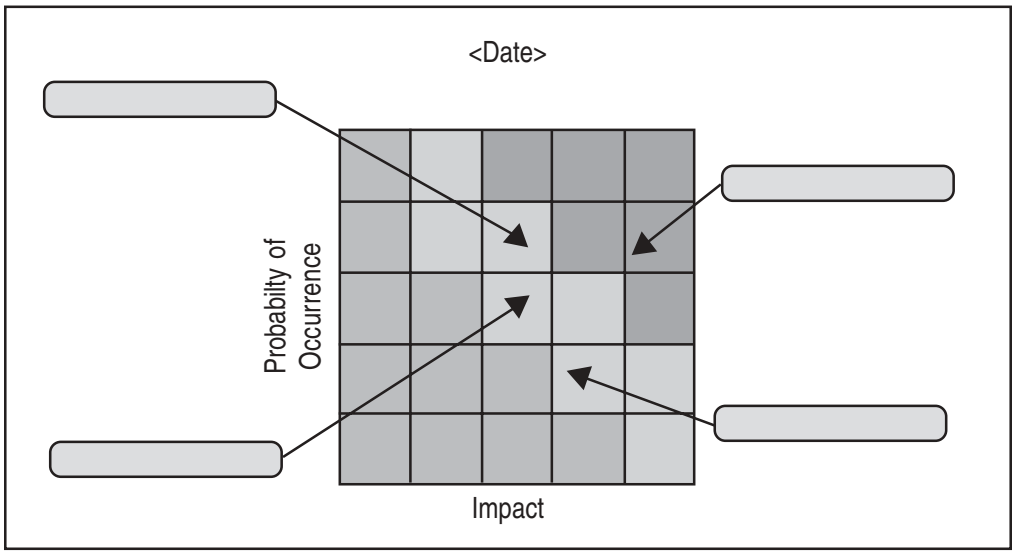


Figure 7. Sample Risk Matrix

probability and impact. By using the previously defined measures for impact in the areas of cost, schedule or technical performance, the team can make a meaningful comparison across these different areas and at least provide an ordinal ranking of the risks. If the impact can be quantified in terms of cost, and the cost of mitigation options included in the analysis, then the program has the information needed to make best use of limited resources.

Figure 8 provides an example of expected value in a simple decision tree. The question is whether or not it makes economic sense to bet $0.50 on one chance in six to win $6.00. The expected value of the chance of winning is $1.00; considering the cost of the bet, the expected value of the decision to play the game is $0.50. Clearly it would make sense to play the game for as long as the casino would allow it. (Do not expect to find this game in Las Vegas.) A programmatic analogy would be to ask if it makes economic sense to fund a $50 thousand prototype of a promising technology that could save the program $600 thousand, assuming there is one chance in six of it being successful.

A related question is to ask, "How much should you to bet?" In Figure 8, the logical answer is to bet no more than $1.00, because this is the "point of indifference," or the point at which the "expected value" for all available options is equal.

Expected Value vs. Realized Cost

In gambling casinos, the games are designed such that the odds are always in favor of the house. If that is true, then why do people play? If the uncertain event actually occurs, it is the "value you expect" that is realized, which is why otherwise rational people buy lottery tickets; the chance of winning is zero if you do not

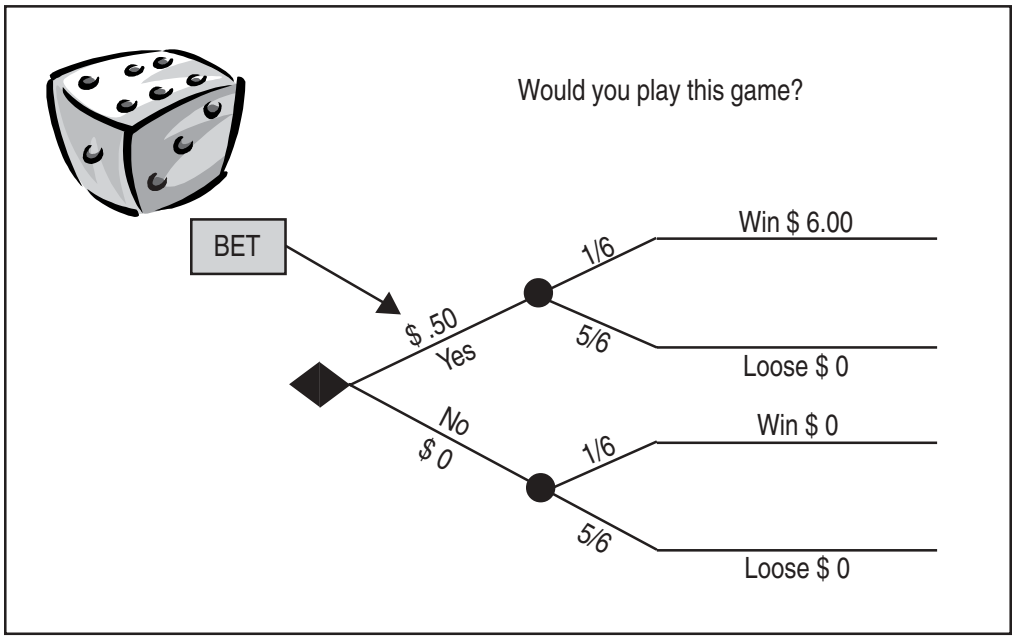


Figure 8. Expected Value in a Simple Decision Tree

play, so why not spend a few bucks on the Powerball Jackpot? This total is the value that contingency planning has to consider. Contingency planning has to be ready to absorb the full impact if the risk event actually occurs.

Risk Tolerance

The example in Figure 8 also illustrates the concept of risk tolerance, or "How much would you be willing to bet?" What if the "house" could stop the game at any time? Would you still play? What if the bet was $5.00 for a chance to win $60.00, $500 to win $6,000, $5 million to win $60 million? How much would you be willing to lose on a single roll of the dice if the game could stop at any time, no matter what the expected value? The greater the risk tolerance, the greater the bet someone is willing to make. The more well funded the program, the greater the opportunity to take advantage of mitigation options.

"Mitigation planning focuses on three things: reducing the probability of the risk event occurring, reducing the impact if it does, and increasing the probability of more acceptable outcomes."

Many programs do not have the resources to invest in expensive mitigation. A low-risk program will have a lower risk tolerance, and it would not be able or willing to invest for only a probable capability. It will want that capability to be more certain, if not already demonstrated.

Understanding Expected Value Can Help Avoid Analysis Paralysis

A decision to bet $0.50 does not take a lot of time or cost to analyze. However, a decision to redesign a major component of a weapon system to improve reliability takes more careful analysis. How much does the reliability have to improve to recover the cost of the improvement and when will the payback occur? A lot of assumptions are involved in generating cost data to support this type of analysis, and the estimates take time and money to prepare. How much is this additional detail worth? If all estimates of the reasonable range for these values produce an expected value to one side of the point of indifference, there is no need for further analysis.

Mitigation Strategies

Risk response activities can be divided into two broad categories: Risk Mitigation and Contingency Planning. The distinction is the difference between expected value and the "value you expect."

Mitigation Planning

Mitigation planning focuses on three things: reducing the probability of the risk event occurring, reducing the impact if it does, and increasing the probability of more acceptable outcomes. These are the things that drive expected value, that mitigation seeks to reduce. One way to reduce the impact is to get someone else to absorb it or to implement an interim solution.

Contingency Planning

Contingency planning focuses on absorbing the impact if a risk event actually occurs. This may be the result of a conscious decision by the program not to take any action to mitigate a risk, or a recognition that the mitigation actions may be ineffective.

Crisis Management — When the Unforeseen Occurs

If you do not practice risk management, you can expect to get a lot of practice at crisis management. But even with a robust and effective risk management program in place, "unknown unknowns" will occasionally (and sometimes dramatically) become "known." Handling these situations requires that four things be in place ahead of time:

1. **Rapid communication capability** with a clear path for passing critical information. It is essential that program management and the resource sponsor have accurate information as quickly as possible. The points of contact who are authorized to speak for the program have to be clearly understood to avoid any confusion.

2. **Established points of contact** in key support organizations, including those that don't normally support the program. Think about the skills that could be needed and know where to obtain this support.

3. **Communication skills** training for key program personnel. In any program where news media may become involved, people in positions who may be asked to conduct interviews should have the benefit of prior training.

4. **Established credibility** with upper management, public affairs, trade press, and other news media. Keep information flowing during normal times so when a crisis occurs, the relationships are established so you do not get too much "help."

Risk Management in Action

How do you set up a risk management program and what do risk managers do? The program manager should assign someone knowledgeable to champion risk management. This is typically someone with direct reporting responsibility to the program manager, and is often the deputy program manager or another senior, knowledgeable person. The risk manager should establish the process, provide training for the team, make it easy to nominate risks, help the team distinguish between risks and issues, and have someone keep records of progress and status.

"A good risk definition will distinguish between the facts of the situation and the uncertain event that is of concern."

Risk Management Board

The program should have a formal board or group focused on managing risk. Whether called a Risk Management Board (RMB), Risk Review Board, Program Risk Advisory Board, or some other designation, the function is the same; it assesses risks that have been nominated and periodically examines the overall program for other risks that may need attention. The RMB typically reports to senior program leadership when there are risks that require a higher level of attention, and works with lower-level teams on nominated and open risks. The risk board is most effective when chaired by someone senior enough

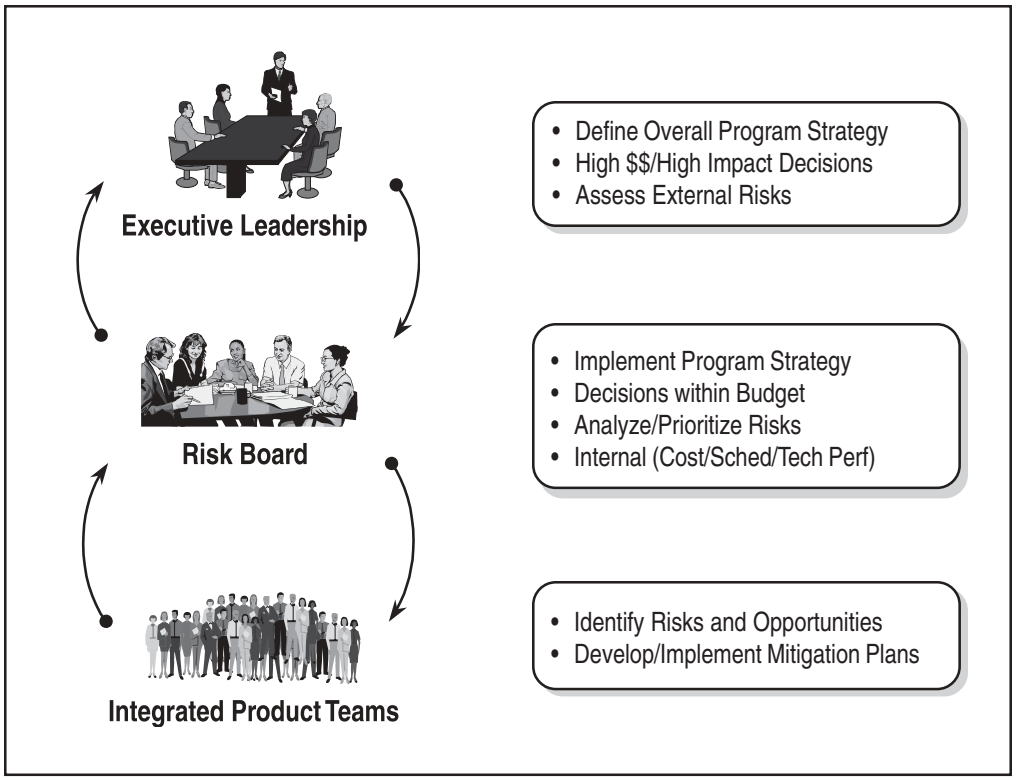


Figure 9. Risk Management Structure

to provide program direction. Figure 9 shows the structure and responsibilities of these boards.

Risk Nomination

When a risk is nominated, the originator needs to provide enough information for the Risk Management Board to determine the outcome. A Risk Nomination Form should be used to ensure consistency and completeness. The earlier definition of Risk had several key words that deserve further attention.

Situation. One of the most effective ways to eliminate risk is to change some of the underlying facts of the situation such that the risk goes away. Identify all factors that are relevant and separate facts from assumptions. Assumptions — which may not be true — are usually a good place to start zeroing in on risks. There is significant partial credit for structuring the problem correctly because this provides the framework for all remaining risk management activities. This is a case where perception is absolutely NOT reality. As illustrated in Figure 10, by including irrelevant information or failing to consider relevant information, the team may mitigate outcomes and impacts that do not really exist and fail to mitigate those that do (A). In severe cases, a team may completely fail to identify the true risk (B).

Uncertainty. A good risk definition will distinguish between the facts of the

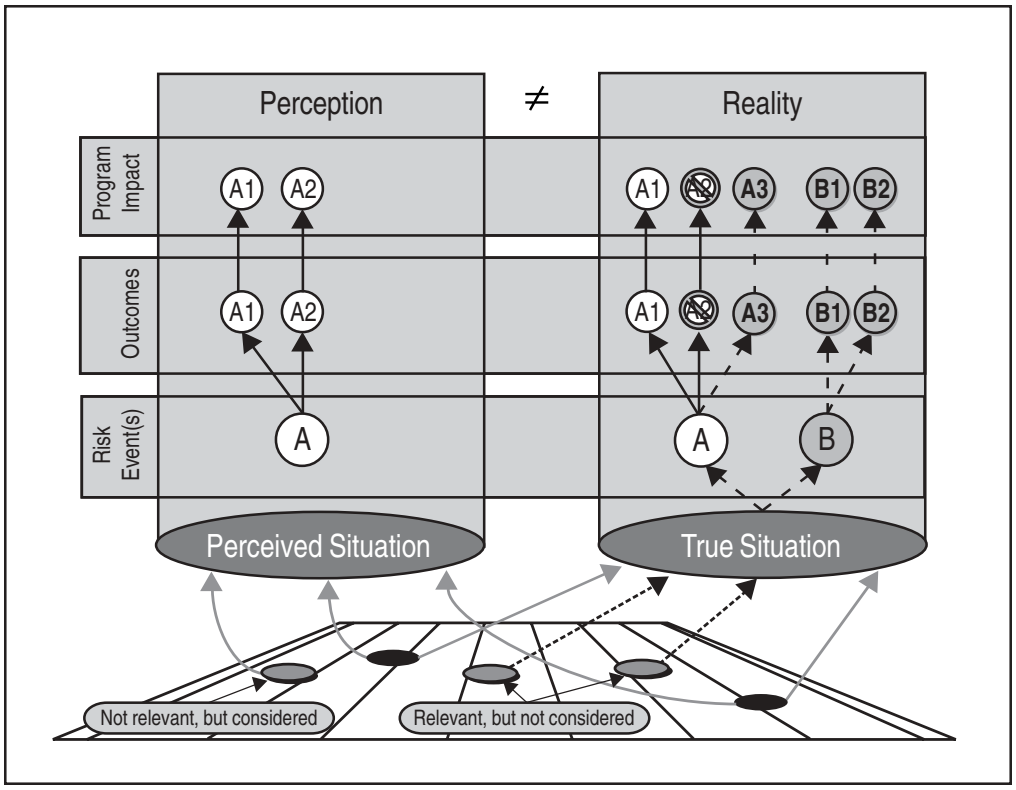


Figure 10. Perception Is Not Reality

situation and the uncertain event that is of concern. If the event is internal to the program, the program team may be able to directly control factors surrounding it. If it is external, then the program team will have to look for ways to influence those factors, or if not, start developing contingency plans.

Do not accept a "noun" as a description of a risk event. "Phase II Staffing" or "Slow Cook-off Test" may be good titles or names for a risk, but they are not good descriptions of the event itself. What exactly about staffing or a particular qualification test might have an impact on the program? It may be an absolute certainty that the Slow Cook-off Test will be performed; the actual risk event is that the existing weapon system design may not pass the test. There is also the chance that, even if it does pass, the Weapon System Explosive Safety Review Board may not approve the weapon for shipboard use based on a single test. Pulling the thread on these details can lead to some very innovative and effective mitigation actions.

Issues Are Not Risks. A key concept is that uncertainty has to exist for a risk to exist. If there is no uncertainty, then it is an issue, not a risk. There is a subtle academic distinction between decisions under Risk and decisions under Uncertainty (Bourd, 1989).

Risk is generally associated with problems for which a statistical basis for

the probability exists. An example would be the risk of accepting bad parts in a production lot based on destructive testing conducted on a statistical sample of those parts.

Uncertainty is when no probabilities exist other than those that may be subjectively assigned. In most cases, program office decision-makers deal with the latter case; we are just not pulling colored jellybeans out of a jar. Since probability should be assessed either analytically or subjectively in all cases, this article intentionally ignores the distinction.

Impact. What are the possible outcomes and impacts? If a risk event occurs, several outcomes may be possible. Each outcome has a distinct probability and impact that should be assessed. Figure 6 shows and defines the items that a risk nomination should include: the Situation, Uncertainty, Impact, and Tasks to Mitigate. It also shows the actions available to the RMB: to accept or reject the risk. If there is no uncertainty involved, the risk should be rejected and handled as an issue.

Tasks To Mitigate. The risk nomination should include a recommendation of the tasks that should be performed to mitigate the risk. Those close enough to the problem to see the risk are often in the best position to recommend ways to avoid or minimize it.

Is Risk Working on Your Program?

Is your program continually reacting to events that could have been foreseen? Are you responding to one crisis after another or planning ahead and proactively managing alternatives? Risk management makes the difference. An effective risk management program is one in which the team is looking ahead and taking effective action to reduce adverse impact to the program. There are several leading indicators that can be checked to provide assurance that the proper risk management activities are being conducted.

Review the Risk Management Plan, minutes of the Risk Management Board, and any reports to senior management. Does the program risk management documentation describe a process that is actually being followed?

There should be a clear link between the documented process, risks nominated and accepted by the board, and risk reports in program briefings.

Summary

Decisions you make do not necessarily determine the future, but they *will* determine the past: make sure it is one you can live with. By actively managing risk, you can create executable options and have alternatives in place that allow the program to survive when — not if — the unforeseen occurs.

REFERENCES

Baird, B.F. (1989). *Managerial decisions under uncertainty: An introduction to the analysis of decision-making.* New York: John Wiley & Sons, Inc.

Hillson, D. (2002, October). Use a risk breakdown structure (RBS) to understand your risks. *Proceedings of the Project Management Institute Annual Seminars & Symposium*, San Antonio, TX.

Bill Shepherd, PMP, works for Booz Allen Hamilton, a global management and technology consulting firm. He is an experienced manager with over 27 years of experience in the U.S. Navy, Joint Service, and commercial project management. While on active duty, he served as deputy program manager for the Joint Standoff Weapon and FA-18 E/F. Shepherd is a Project Management Professional (PMP) and teaches Booz Allen's internal project management course.
(E-mail address: Shepherd_bill@bah.com)